ZEROFOX INTELLIGENCE

Flash

Cyberattacks on European Airports Reveal Contagion Risk

F-2025-09-22a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, Threat Actor, Aviation

September 22, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on September 22, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cyberattacks on European Airports Reveal Contagion Risk

| Key Findings

- Over the weekend of September 19–21, 2025, a cyberattack caused widespread operational disruption at major European airports, resulting in a host of flight cancellations and delays.
- As of writing, no threat actor has claimed responsibility for the attack. The attribution details—such as the ransomware strain or the threat actor responsible—have not yet been made public, and it remains unclear whether a third-party vendor or Collins Aerospace itself was targeted.
- This attack highlights a critical vulnerability in the IT infrastructure used in the aviation industry, especially where third-party systems support multiple airports and airlines.
- The airline industry likely faces significant pressure to quickly meet ransomware demands, as customer satisfaction and maintaining scheduled flight times are crucial to its business model.

Details

Over the weekend of September 19–21, 2025, a cyberattack caused widespread operational disruption at major European airports, resulting in a host of flight cancellations and delays. The attack reportedly targeted the Multi-User System Environment (MUSE) passenger processing software provided by Collins Aerospace, forcing airlines and ground services to revert to manual check-in and boarding procedures.[1]

- On September 22, 2025, the European Union Agency for Cybersecurity (ENISA) confirmed that the cause of the disruption was a ransomware attack but did not confirm the threat actor behind it.[2]
- Collins Aerospace is a U.S.-based aviation and defense technology company—with a global presence at more than 170 airports—that offers solutions for passenger processing and facilitation, airport operations, and baggage management.[3]

In a statement to *Reuters*, RTX Corporation (formerly Raytheon Technologies Corporation), the parent company of Collins Aerospace, stated that it was aware of the cyber disruptions at certain airports without specifying which ones; however, several airports in the region have since reported being affected by the software disruptions. As of writing, Heathrow Airport in London (Europe's busiest airport), Brussels Airport, Berlin Brandenburg Airport, Dublin Airport, and Cork Airport have revealed varying degrees of impact.[4]

In previous systems, each airline managed its own dedicated service area in an airport, making access singular and contained to the airline itself. However, in recent years, concerns regarding efficiency have caused several airports to shift toward newer systems like MUSE, a shared-use platform that integrates passenger records, baggage

[1] hXXps://www.csoonline[.]com/article/4060804/european-airports-continue-to-crawl-after-a-cyberattack-on-collins-muse-systems.html
[2] hXXps://www.aa[.]com[.]tr/en/europe/eu-cybersecurity-agency-confirms-ransomware-attack-behind-airport-disruptions/3694832
[3] hXXps://www.collinsaerospace[.]com/what-we-do
[4] hXXps://www.reuters[.]com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/

details, and security requirements into one digital platform used across airlines to enable dynamic desks and gates within airports.[5]

- This change underpins the increased likelihood of vulnerabilities to European aviation, as an attack on one entity could take out multiple airports, unlike the previous system, wherein threat actors would only be able to target airlines individually.
- As a result of MUSE's compromise, every airline in an impacted airport likely could not access their shared digital framework, forcing them to rely on often cumbersome and time-consuming manual check-ins.
- Due to the check-in disruptions, several airports experienced subsequent delays and flight cancellations, which are likely to persist if airlines continue to experience prolonged digital limitations.

As of writing, no threat actor has claimed responsibility for the attack. The attribution details—such as the ransomware strain or the threat actor responsible—have not yet been made public, and it remains unclear whether a third-party vendor or Collins Aerospace itself was targeted. There is currently no evidence to suggest a data breach has taken place or that passenger data has been compromised; however, digital forensic analysis is reportedly ongoing.[6]

It is likely that some of the aforementioned airports will continue to experience delays and disruptions in the coming days, as efforts are still ongoing to restore the affected systems. This attack highlights a critical vulnerability in the IT infrastructure used in the aviation industry, especially where third-party systems support multiple airports and airlines. The airline industry likely faces significant pressure to quickly meet ransomware demands, as customer satisfaction and maintaining scheduled flight times are crucial to its business model. It is likely that airport authorities and affected airlines will face pressure to reassess cyber resilience standards and supply chain risk management as a result of this attack.

5

hXXps://www.techtimes[.]com/articles/312010/20250920/software-behind-europes-check-chaos-what-muse-why-it-matters.html

6

hXXps://www.reuters[.]com/business/aerospace-defense/european-airports-race-fix-check-in-glitch-after-hacking-disruption-2025-09-21/

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi-factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%